7-Ч

УДК 004.9

В.М. Чаплига, О.А. Нємкова
Львівський інститут банківської справи
Університету банківської справи
Національного банку України
Україна, 79058, м. Львів, проспект В. Чорновола, 61

Сучасні рішення проблем витоку інформації фінансових установ

V.M. Chaplyga, E.A. Nemkova
Lviv Institute of Banking of the University of Banking
of the National Bank of Ukraine, c. Lviv
Ukraine, 790588, c. Lviv, boulevard V. Chornovola, 61.

Modern Solutions to the Problem of Information Leakage at Financial Institutions

В.М. Чаплыга, Е.А. Немкова
Львовский институт банковского дела
Университета банковского дела
Национального банка Украины
Украина, 79058, г. Львов, проспект В. Черновола, 61

Современные решения проблем утечки информации финансовых учреждений

У статті наведено аналіз сучасних систем захисту від витоку інформації, що можуть бути використані в першу чергу у фінансових установах. Розглянуто тенденції розвитку та вдосконалення систем внутрішньої інформаційно-технічної безпеки. Запропоновано способи вдосконалення засобів запобігання витоку.
Ключові слова: інсайдер, контур інформаційної безпеки, витік інформації.

In the article, modern systems of protection against information leaks, which can be primary used at financial institution, are analyzed. The trends in the development and improvement of internal systems of information technology security are considered. Improvements to facilities to prevent leaks are proposed.
Key words: insider, the contour of information security, information leakage.

В статье проанализированы современные системы защиты от утечки информации, которые могут быть использованы в первую очередь для финансовых учреждений. Рассмотрены тенденции развития и усовершенствования систем внутренней информационно-технической безопасности. Предложены способы усовершенствования средств для предотвращения утечек.
Ключевые слова: инсайдер, контур информационной безопасности, утечка информации.

Вступ

Питання інформаційної безпеки в наш час, коли фактично жодна обробка даних не відбувається без участі комп’ютерів, постають практично для будь-якої компанії чи установи, незалежно від форми її власності та роду занять. Відкритість сучасних комп’ютерних систем, їх складність, а також загальна комп’ютерна грамотність ще більше загострюють ці питання. Стрімкий розвиток інформаційних систем та технологій, їх широке впровадження на підприємствах, що найбільш чутливі до витоку

конфіденційної інформації, сприяють такому негативному явищу, як інсайдер. До недавнього часу основна увага в області IT-безпеки була зосереджена на боротьбі проти вірусних атак, а також небезпек, що пов’язані з Інтернет-мережею. У результаті було створено багато антивірусних продуктів, бази яких щоденно оновлюються; поштові клієнти навчились боротись зі спамом; брандмауери захищають локальні мережі фірм від різноманітних видів інтернет-шахрайства. Але останніми роками виявилось, що існує ще один від небезпеки, на який спочатку зовсім не звертали увагу – це витік інформації із фірми. Поняття «інсайдер» набуло важливого значення.

Банки та фінансові установи, що опрацьовують персональні дані населення, є тими підприємствами, для яких порушення конфіденційності інформації та її витік вважаються найбільшою загрозою. Кожен витік інформації із компанії має два типи наслідків. По-перше, це втрата конкурентних переваг, тому що конкуренти отримують чи клієнтські бази, чи технологічне ноу-хау, чи маркетинговий план та інше. По-друге, витік інформації погіршує імідж компанії, що приводить до втрати 20 – 25% прибутку. Тому для банків України питання інформаційної безпеки сьогодні піднесено на законодавчий рівень [1-4]. Як показує статистика [5-7], найбільше фінансові установи потерпають саме від інсайдерів. Враховуючи нестабільність сучасного суспільства, хвилі економічних криз, багато співробітників у побоюванні бути звільненими або наперед запасаються цінною інформацією, або під час своєї роботи займаються продажем конфіденційних даних. Компанія InfoWatch свідчить [8], що приблизно 60% звільнених співробітників залишають у себе цінні дані підприємства, причому основні витоки найбільш цінних активів припадають на фінансову кризу 2008 – 2009 років. Як очікують економісти Всесвітнього банку, ризик нової кризи призведе до скорочення штату працівників, тобто збільшення витоку конфіденційної інформації.

Обійтись тільки адміністративними мірами для запобігання IT-інцидентів, пов’язаних із витоком інформації, на сьогоднішній день вже не вдається. Справа тут не тільки в збільшенні обсягів та різноманіття цінної інформації, а в принциповій відкритості інформаційних систем фінансових установ. Тому стрімкий розвиток отримують системи DLP (Data Leakage Prevention), які знаходять та блокують несанкціоноване передавання конфіденційної інформації по будь-якому каналу з використанням інформаційної структури підприємства. Основна задача цих систем – це мінімізація ризику витоку або знищення даних, промислового шпигунства, недбалості та інших неправомірних дій співробітників відносно корпоративної інформації. Системи DLP, або Контур інформаційної безпеки (КІБ) (ця назва застосовується на теренах СНД), – це потужні інтелектуальні системи, в першу чергу завдяки використовуваним технологіям детектування, а також управлінню системою моніторингу та обробки інцидентів.

Важливі питання для власників успішного бізнесу: «Як захистити свій бізнес? Як захистити найбільш важливу комерційну інформацію? Кому довіряти?» – були, є та будуть поставати з часом все гостріше. Тому створити систему інформаційної безпеки або покращити вже існуючу завжди вигідно і ніколи не пізно.

Суттєві втрати відбуваються через неакуратне ставлення персоналу до інформації, а цей фактор не так легко усунути. До того ж більшість людей є беззахисними проти методів соціальної інженерії, яка маніпулює або людскою недбалістю, а частіше – їх прагненням зробити як краще, непомітно порушуючи при цьому посадові інструкції. Тому впровадження КІБ для багатьох підприємств, особливо банків та інших фінансових установ, є виходом з положення для запобігання витоку конфіденційної інформації.

Слід відзначити ще одну важливу тенденцію. Чим більша компанія чи установа і чим глибше впроваджені комп’ютерні технології в бізнес-процеси, тим сильніше її IT-безпека залежить від інсайдерів.

Наведемо декілька цифр, які свідчать про необхідність боротьби з явищем інсайдера. З року в рік збитки в результаті витоку персональних даних та конфіденційної інформації зростають на 20 – 25%. У 2006 році економіка США втратила $ 500 млрд від таких інцидентів. Якщо врахувати сукупні втрати світової економіки від витоку комерційних таємниць, то отримаємо величину у $ 175 млрд. Тобто сумарні втрати щорічно складають майже $ 700 млрд. Інфляція та щорічне зростання збитків на 20 – 25% наближають цю цифру до $ 1 трлн.

Метою даної роботи є аналіз сучасних систем захисту від витоку інформації фінансових установ, а також виявлення тенденцій розвитку та вдосконалення систем внутрішньої ІТ-безпеки.

Аналіз сучасних систем захисту від витоку інформації

Усвідомлення проблеми інсайдерів можна віднести до 2004 – 2006 років, коли в результаті опитувань великого числа компаній по всьому світу, зокрема такі дослідження проводила InfoWatch – експерт в області систем забезпечення інформаційної безпеки, з'ясувалося, що більше половини всіх інцидентів в області ІТ-безпеки (60%) відбулося саме з провини інсайдерів. Сучасний аналіз інсайдерських загроз показує, що фінансові компанії та держструктури постійно стикаються з внутрішніми загрозами. Варто навести декілька прикладів інцидентів, що відбулися за останній час [8]:

– Управління Роскомнагляду по Санкт-Петербургу і Ленінградській області прийшло до висновку, що ТОВ «Вконтакте» порушило законодавство про персональні дані. До ТОВ «Вконтакте» буде застосовано адміністративні та штрафні санкції (від 15.06.2012).

– Великобританія. Міська влада Глазго принесла вибачення перед громадянами та юридичними особами, чиї дані зберігались на викрадених ноутбуках. Всього скомпрометовано 37 тис. персональних даних (від 14.06.2012).

– США. Федеральна кредитна спілка Bethpage (BFCU) повідомила 86 тис. власних клієнтів про компрометацію інформації по їх кредитних картках (від 13.06.2012).

– В рунеті з'явилась новина про крадіжку паролів користувачів LinkedIn (від 07.06.2012).

– Співробітник компанії JPMorgan Chase &Co в Японії був визнаним у розголошенні інсайдерської інформації, що пов'язана з продажем акцій компанії Nippon Sheet Glass Co 2012 р. (від 31.05.2012).

– Організація, що надає медичні послуги населенню, Durham Region Health, заплатить штраф у 500 тис. доларів через три роки після витоку інформації (від 29.05.2012).

При обговоренні систем захисту інформації від витоку прийнято поділяти інсайдерів на типи. InfoWatch виділяє шість типів інсайдерів (табл. 1). Зауважимо, що мова йде про витік саме з корпоративної мережі, а не про такий витік інформації, коли даних небагато, і тому інсайдеру не потрібно використовувати мережу – він у змозі запам'ятати кілька цифр або речень.

Таблиця 1 – Характеристика типів інсайдерів

Тип інсайдера	Намір	Користь від витоку	Мета, хто ініціатор витоку	Дії при неможливості виконання	Ефективні запобіжні дії
Халатний (необачний, дуже неуважний) Ненавмисний	Немає	Немає	Немає	Повідомлення системному адміністратору або керівництву	Контентна фільтрація вихідного трафіка у сукупності з менеджерами пристроїв введення-виведення

Продовження табл. 1

Такий, ким маніпулюють (жертви соціальної інженерії) Ненавмисний	Немає	Немає	Немає	Повідомлення системному адміністратору або керівництву	
Ображений Навмисний	Має	Немає	Має, сам	Скеровує дії на інший об’єкт, наприклад, фальсифікацію або знищення інформації	Організаційні та правові міри у сукупності з менеджерами пристроїв введення-виведення, контентна фільтрація внутрішньої мережі, шифрування систем резервного копіювання
Нелояльний Навмисний	Має	Немає	Має, сам	Імітує виробничу необхідність	
Такий, що підзаробляє Навмисний	Має	Має	Має, сам або зовнішній замовник	Відмова/ імітує виробничу необхідність/ взлом	
Засланий Навмисний	Має	Має	Має, зовнішній замовник	Взлом	

Вивчення типів інсайдерів має прямий практичний сенс, тому що це визначає методи боротьби з інсайдерськими загрозами, блокування конкретних комунікаційних каналів, проведення організаційної роботи зі співробітниками. Фактично це визначає обсяг робіт та їх вартість, що потрібно витратити для гарантування безпеки. Як показує аналіз характеристик, умовно інсайдерів можна поділити на навмисних та ненавмисних. Виявляється, що у своїй діяльності вони користуються різними каналами витоку. Якщо провести порівняння (дані за 2011 рік) між використанням різних каналів витоку навмисними та ненавмисними інсайдерами, то отримаємо наступне (табл. 2).

Таблиця 2 – Канали витоку у використанні навмисними та ненавмисними інсайдерами

Канал витоку	Навмисні інсайдери, %	Ненавмисні інсайдери, %
Паперові носії	17	23
ПК, сервери	15	11
WEB, інтранет	8	22
Носії резервних копій	8	6
Ноутбуки, смартфони	6	12
З’ємні носії	5	8
Електронна пошта	3	10
Не визначено + інші	27 + 11	4 +4

Аналізуючи дані табл. 2, відзначимо, що вищезгадані DLP системи ефективно протидіють ненавмисним інсайдерам. Для запобігання діям навмисних інсайдерів можливостей таких систем недостатньо, все залежить від рівня обізнаності інсайдера та кваліфікації спеціалістів з інформаційної безпеки. Як правило, DLP системи надають можливість проаналізувати ситуацію у випадку, коли витік відбувся. Звичайно, ідеальна система інформаційної безпеки прагне взагалі не допустити ситуації витоку.

Треба зазначити, що навмисні інсайдери навчились обходити DLP системи, тобто хоча витік відбувається, система його не реєструє. Цей висновок зовсім не означає, що від подібних систем захисту слід відмовитись, тому що залишається така складова, як ненавмисні інсайдери, з якими DLP системи справляються чудово. Аналітика витоків за роками показує, що відношення навмисних витоків до ненавмисних складає 42% до 43%, тобто кількість їх практично збігається. Наприкінці аналізу інсайдерської діяльності слід відзначити, що за останніх два роки сумарна кількість інцидентів по всьому світу практично не змінилася: 2011 рік – 801, 2010 рік – 794, 2009 рік – 747 (дані відображають тільки ті витоки, що стали офіційно відомі, за оцінками складає це приблизно 1% від кількості всіх витоків), що можна віднести на рахунок початку ефективного впровадження DLP систем.

Розглянемо більш детально конкретну систему запобігання витоку інформації, а саме Контур інформаційної безпеки від SearchInform (КІБ). Насамперед треба відзначити, що КІБ – одне з найбільш універсальних і практичних рішень з контролю за інформаційними потоками підприємства на всіх рівнях – від комп'ютера кожного окремого користувача до серверів локальної мережі. Контролюються усі дані, що йдуть в Інтернет. Контур має модульну структуру, тобто замовник може за власним вибором встановити тільки частину компонентів.

У методології КІБ реалізований принцип захисту каналів витоку. Кожний канал контролюється специфічним пошуковим механізмом – сніфером, налаштованим тільки на даний канал. Вся інформація перехоплюється, обробляється та зберігається в базі даних SQL-типу, увійти в яку може тільки офіцер безпеки. Управляє КІБ також тільки офіцер безпеки. Він знає паролі входу (системний адміністратор їх не знає), налаштовує пошукові механізми, отримує інформацію про інциденти.

До числа модулів контуру входять [9]:

– DataCenter – центр управління всіма індексами (механізм специфічного архівування файлів з метою зберігання та пришвидшення пошуку), створеними компонентами КІБ. DataCenter дозволяє розбивати індекси на частини, збільшуючи продуктивність пошуку інформації; задавати правила створення нових індексів за певний інтервал часу. Це надає можливість відстежувати інформацію тільки за необхідні періоди часу, а також слідкувати за станом роботи всіх компонентів КІБ і відсилати повідомлення на вказаний e-mail (наприклад, офіцера безпеки) при будь яких інцидентах.

– Сервер індексації робочих станцій дозволяє в режимі реального часу відслідковувати появу конфіденційної інформації на комп'ютерах користувачів і в інших місцях, для цього не призначених (корпоративна мережа).

Набір сніферів (агентів), кожен з них контролює свій канал передачі інформації:

– PrintSniffer дозволяє перехоплювати вміст документів, відправлених користувачем на друк.

– DeviceSniffer перехоплює інформацію, яка записується на різні зовнішні пристрої (наприклад USB-флешки, CD/DVD диски).

– MailSniffer перехоплює всю вхідну і вихідну електронну пошту.

– SkypeSniffer перехоплює голосові та текстові повідомлення Skype.

– IMSniffer перехоплює повідомлення інтернет-пейджерів (ICQ, QIP та інші).

– HTTPSniffer дозволяє перехоплювати інформацію, що відправляється в інтернет-форуми, блоги та інші web-сервіси.

– AlertCenter – це «мозковий центр» всієї системи безпеки. AlertCenter – самостійний додаток, що опитує всі перераховані агенти і за наявності в перехопленій інформації певних ключових слів, фраз або фрагментів тексту негайно сповіщає офіцера безпеки.

Перехоплення даних здійснюється або сервером NetworkSniffer, або агентами, встановленими на цільові робочі станції користувачів:

– сервер NetworkSniffer слухає мережний трафік і перехоплює документи користувачів на рівні мережного адаптера. Така схема реалізована для компонентів MailSniffer, IMSniffer, HTTPSniffer;

– агенти встановлюються на робочі станції користувачів і перехоплюють документи користувачів безпосередньо на робочих станціях. Така схема роботи застосовується для компонентів SkypeSniffer, DeviceSniffer, PrintSniffer, Сервер індексації робочих станцій.

Пошукові клієнти дозволяють переглянути всі перехоплені документи з можливістю зрізу по даті і користувачам домену. Схема розміщення компонентів КІБ та напрями інформаційних потоків наведено на рис. 1 [10].

До суттєвих плюсів КІБ слід віднести можливість його встановлення віддалено, що робить можливим швидке встановлення при мінімальній участі системного адміністратора компанії.

КІБ комплектується потужним пошуковим модулем. У ньому реалізовані такі типи пошуку:

1. Пошук за словами з урахуванням морфології та синонімів. Це найпростіший вид пошуку, що дозволяє знаходити документи, які містять шукані слова, їх словоформи і синоніми, незалежно від того, в якому місці документа вони знаходяться.

2. Пошук за фразами з урахуванням порядку слів і відстані між ними. При пошуку інформації нерідко потрібно аналізувати документ не за окремими словами, а за словосполученнями (наприклад, прізвища-імені). У цьому випадку фразовий пошук має очевидні переваги, а саме можливість задати порядок слів і відстань між ними.

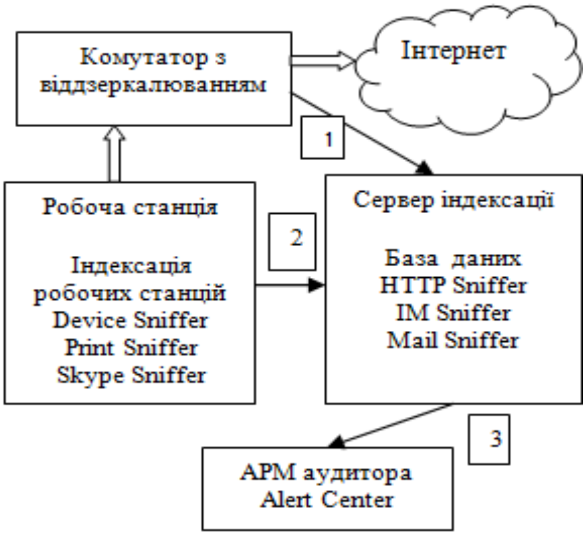


Рисунок 1 – Схема інформаційних потоків: 1 – перехоплення інтернет-трафіка, 2 – передача інформації агентами в базу, 3 – передача повідомлень аудитору

3. Пошук регулярних виразів. Такий пошук дозволяє відстежити послідовності символів, характерні, скажімо, для персональних даних, фінансових документів або структурованих записів у базах даних. Наприклад, система відреагує на спробу відправки запису з такими персональними даними, як прізвище людини, її день народження, номери кредитних карт, телефони та інше.

4. Пошук за цифровими відбитками. Цей вид пошуку передбачає визначення групи конфіденційних документів і зняття з них цифрових відбитків, за якими в подальшому і буде здійснюватися пошук.

5. Запатентований алгоритм «Пошук подібних». Інтелектуальні можливості цього типу пошуку дозволяють відстежувати відсилання конфіденційних документів навіть у тому випадку, якщо вони були попередньо відредаговані. Як пошуковий запит використовуються як фрагменти документів, так і документи цілком. Результатом пошуку є документи, що або містять пошуковий запит цілком, або схожі на нього за змістом.

Тенденції розвитку систем внутрішньої ІТ-безпеки

При обговоренні тенденцій розвитку систем внутрішньої ІТ-безпеки будемо в основному спиратись на необхідність таких систем для боротьби із навмисними інсайдерами. Для цього потрібно мати портрет такого інсайдера, уявляти область його інтересів і орієнтуватись на можливі канали витоку, що ним використовуються.

Наведемо типовий портрет навмисного інсайдера. У 98% випадків це є чоловік незалежно від віку, соціального статусу та раси. Як правило, без кримінального минулого. Основна мотивація – образа на когось, хто асоціюється з установою. У половині випадків такий інсайдер є вже звільненим, але досі має доступ до інформаційних ресурсів (47%). Практично всі інсайдери є спеціалістами, що пов’язані з ІТ-технологіями. Серед них 38% – системних адміністраторів, 21% – програмістів, 14% – інженерів, 14% – спеціалістів по ІТ.

Можна зробити висновок про високий рівень технічної підготовки навмисних інсайдерів, тобто ефективними будуть запобіжні заходи, що пов’язані із криптографічним захистом інформації, причому парольну інформацію слід розподіляти між кількома особами, більшість з яких не входить у групи ризику. Дійсно, останнім часом спостерігається тенденція партнерства між виробниками DLP систем та компаніями, що займаються шифруванням та архівуванням електронної пошти.

Серед найбільш привабливих ресурсів банків для інсайдерів виділяють такі [11]:

– скорингові системи, що використовуються для оцінки кредитоспроможності постачальників як в рамках експрес-кредитування, так і для ухвали рішення про кредитування на великі суми;

– унікальні ІТ-розробки, наприклад по системі інтернет-банкінгу;

– база залишків по рахунку (для спроб використання з метою шантажу або шахрайських дій з рахунками заможних клієнтів).

Відомо, що ця інформація зберігається у незашифрованому неструктурованому вигляді. Тенденцією в цьому аспекті є збільшення кількості форматів, реалізованих у мережних рішеннях DLP систем, а також у встановленні правил і типів шифрування для кожної фінансової установи залежно від груп користувачів та виду ресурсу.

Цілісної системи внутрішньої ІТ-безпеки на сучасному етапі не існує. Коротко зупинимось на механізмах і способах запобігання витоку. По-перше, це системи виявлення та попередження витоку. Ці системи добре працюють у країнах, в яких робочою є англійська мова. У зв’язку із загальними тенденціями глобалізації ці рішення переносяться на країни з більш складними мовами. Фільтри, що працюють із інсайдерськими сигнатурами, в даному випадку не підходять. Наприклад, для російської мови використовують шість різних кодувань, до того ж в цій мові майже мільйон словоформ. Загальна тенденція у цьому випадку – пошук нових механізмів фільтрації контенту, так, в КІБ застосовується лінгвістичний та морфологічний аналіз. Для протидії витоку потрібні організаційні заходи, які полягають у проведенні регулярних тренінгів персоналу, створення нормативної бази конфіденційної інформації установи – політики безпеки поводження з різноманітними документами відповідно до категорії конфіденційності і правил роботи з нею.

Другою групою засобів є засоби внутрішнього контролю – Internal Controls. Ця група має справу зі створенням ефективної системи внутрішнього контролю і проходженням зовнішнього щорічного аудиту. Наприклад, американські закони передбачають сувору відповідальність за невиконання таких вимог – $25 млн або 20 років позбавлення волі. Аналогічні положення є в інших нормативних актах Євросоюзу, Росії, Британії. Відмінність від американського законодавства полягає у добровільності виконання положень. У цьому ж криється разюча відмінність у кількості інцидентів, що приходяться на різні країни. Якщо у США повідомлення про інцидент є обов'язковим для компанії, то в Україні, наприклад, це зовсім не так. Тому тенденцією у галузі права по відношенню до витоків є прийняття більш жорстких актів та високої відповідальності керівництва.

Третьою групою засобів підвищення інформаційної безпеки є застосування систем сильної автентифікації. Відомо, що найслабшою автентифікацією є пред'явлення системі паролю або піну. Якщо врахувати, що сьогодні кожний середній користувач повинен пам'ятати приблизно 15 паролів, стає зрозумілим, що такий захист не є сильним – паролі виявляються надто слабкими. Наступний рівень автентифікації – це пред'явлення системі електронного ключа або смарт-карти. Третій рівень – пред'явлення біометріки. Використання багатофакторної автентифікації дозволяє знизити фінансові втрати та мінімізує ризик ІТ-безпеки. На сьогоднішній день популярністю користуються USB-токени, які дозволяють впроваджувати юридично значимий електронний документообіг. Ще одним засобом із цієї серії є електронний підпис, який вже впроваджено в банках для проведення безпечних транзакцій. Тенденція поширення електронного підпису в документообігу натикається на чисто фізичні обмеження центрів сертифікації, які на сьогодні не в змозі надати сертифікати ключів всім бажаючим.

До четвертої групи засобів відносяться системи попередження нецільового використання ІТ-ресурсів. Тенденцією розвитку даної групи є пошук більш інтелектуальних фільтрів, ніж сигнатурний. Фактично це задача штучного інтелекту, вочевидь, її розвиток ще у майбутньому.

До п'ятої групи відноситься архівування корпоративної кореспонденції. Треба відмітити, що міжнародні нормативні акти потребують наявності центрального архіву корпоративної кореспонденції. Аналіз вхідної та вихідної пошти є ефективним методом для розслідування будь-яких корпоративних інцидентів, а також у випадку юридичних претензій можуть бути використані як доказ. Системи архівування вихідної кореспонденції, як правило, включені до складу DLP систем, структура архіву будується на принципах поділу за користувачами. Під'єднання до цього архівування вхідної кореспонденції не є проблемою.

Висновки

Рішення проблем, пов'язаних з витоком інформації в першу чергу для фінансових установ повинні бути комплексними, тому що на сьогоднішній день єдиної системи ефективного запобігання витокам не існує. Проти ненавмисних інсайдерів добре спрацьовують DLP системи, або КІБ. Хоча ці системи постійно вдосконалюються, тим не менш при впровадженні їх у корпоративну мережу можна отримати гарні результати.

Фінансові установи для впровадження КІБ повинні мати чітко розроблену політику безпеки, суттєвою складовою якої є класифікація всієї документації установи на конфіденційну інформацію та інформацію з відкритим доступом.

Використання КІБ доцільно не тільки у фінансових установах та міністерствах і відомствах, а також в компаніях, що працюють з персональними даними (медичними закладами, пенсійними фондами, фірмами мобільного зв’язку, податкової служби), або є власниками цінної технологічної інформації (фармацевтичні фірми, будівельні компанії, фірми, що пов’язані з технологіями виробництва харчової продукції).

Для успішної протидії навмисним інсайдерам слід використовувати комплекс технічних, криптографічних, організаційних та правових засобів. Ця задача повинна вирішуватись як на рівні установи, так і на законодавчому рівні країни. Тенденції розвитку сучасних систем запобігання витоку також вимагають багаторівневих рішень.

Література

1. СОУ Н НБУ 65.1 СУІБ 1.0:2010. Методи захисту в банківський діяльності. Система управління інформаційною безпекою. Вимоги (ISO/IES 27001:2005, MOD). – 67 с.
2. СОУ Н НБУ 65.1 СУІБ 2.0:2010. Методи захисту в банківський діяльності. Звід правил для управління інформаційною безпекою (ISO/IES 27001:2005, MOD). – 209 с.
3. «Про набрання чинності стандартам з управління інформаційною безпекою в банківський системі України» [текст] : постанова правління НБУ від 28.10.2010 р. № 474.
4. Єпіфанов А.О. Базель ІІ: проблеми та перспективи використання в національних банківських системах / А.О. Єпіфанов, І.О. Школьник, П. Райхлінг. – Суми : ДВНЗ «УАБС НБУ», 2011. – 261 с.
5. Арсентьев А. Социальные сети: киберпреступники ставят ловушки на СМБ [Электронный ресурс]. – Режим доступа : http://www.cnews.ru/news/top/index.shtml?2011/03/02/430417.
6. Риск социальных сетей для малого бизнеса [Электронный ресурс]. – Режим доступа : http://web-by.+com/social_nets.
7. Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности / В.А. Курбатов, В.Ю. Скиба. – СПб. : Питер, 2008. – 320 с.
8. Електронний ресурс. – Режим доступу : www.infowatch.ru.
9. Контур інформаційної безпеки. Керівництво аудитора безпеки. – 2010, SearchInform [Електронний ресурс]. – Режим доступу : http://searchinform.ru/.
10. Чаплига В.М. Особливості впровадженні контуру інформаційної безпеки SearchInform / В.М. Чаплига, О.А. Нємкова // Системи обробки інформації. – 2012. – Вип. 4 (102). – Т. 2 – С. 82-86.
11. Якуб’як І. Особливості захисту фінансової інформації як складової фінансової безпеки комерційних банків / І. Якуб’як, О. Максимук, М. Марчук // Захист інформації і безпека інформаційних систем : матеріали І Міжнародної науково-технічної конференції. – Львів : НУ ЛП, 2012. – С. 20-21.

Literatura

1. SOU N NBU 65.1 SUIB 1.0:2010 “Metody zahystu v bankivs’kij dijal’nosti. Systema upravlinnja informacijnoju bezpekoju. Vymogy” (ISO/IES 27001:2005, MOD). 67 s.
2. SOU N NBU 65.1 SUIB 2.0:2010 “Metody zahystu v bankivs’kij dijal’nosti. Zvid pravyl dlja upravlinnja informacijnoju bezpekoju” (ISO/IES 27001:2005, MOD). 209 s.
3. Pro nabrannja chynnosti standartam z upravlinnja informacijnoju bezpekoju v bankivs’kyj systemi Ukrainy. Postanova pravlinnja NBU vid 28.10.2010r. № 474.
4. Jepifanov A.O. Bazel’ II: problemy ta perspektyvy vykorystannja v nacional’nyh bankivs’kyh systemah. Sumy:DVNZ “UABS NBU” 2011. 261 s.
5. Arsent’ev A. Socia’'nye seti: kiberprestupniki stavjat lovushki na SMB.
6. http://www.cnews.ru/news/top/index.shtml?2011/03/02/430417.
7. Risk social’nyh setej dlja malogo biznesa. http://web-by.+com/social_nets.
8. Kurbatov V.A. Rukovodstvo po zashhite ot vnutrennih ugroz informacionnoj bezopasnosti. SPb.: Piter. 2008. 320 s.
9. www.infowatch.ru.
10. Kontur informacijnoi bezpeky. Kerivnyctvo audytora bezpeky. 2010. SearchInform. http://searchinform.ru/.
11. Chapliga V.M. Systemy obrobky informacii. 2012. Vypusk 4 (102). Tom 2. S. 82-86.
12. Jakub’jak I. “Zahyst informacii i bezpeka informacijnyh system” materialy I Mizhnarodnoi naukovo-tehnychnoi konferencii. L’viv: NU LP. 2012. S.20-21.

RESUME

V.M. Chaplyga, E.A. Nemkova

Modern Solutions to the Problem of Information Leakage at Financial Institutions

In the article, modern systems of protection against information leaks, which can be primary used at financial institution, are analyzed. The trends in the development and improvement of internal systems of information technology security are considered. Improvements to facilities to prevent leaks are proposed.

Financial institutions for introduction of contour of information security (KIS) must have the expressly developed policy of safety, the substantial constituent of which is classification of all document of establishment on confidential information and information with the opened access.

Use of KIS is expediently not only in financial institutions and ministries and departments, and also in companies, which work with the personal information (medical establishments, pension funds, firms of mobile communication, tax service), or are the proprietors of valuable technological information (pharmaceutical firms, build companies, firms, that the productions of food goods related to technologies).

KIS has to wide spectrum of preventive actions in relation to the source of confidential information and can be successfully produced with the threats of source of information, when the problem is unintentional insiders. A functional of the contour is carefully thought out, requirements to “iron” are not high and on forces almost all establishments which worry about own defense.

Стаття надійшла до редакції 05.06.2012.